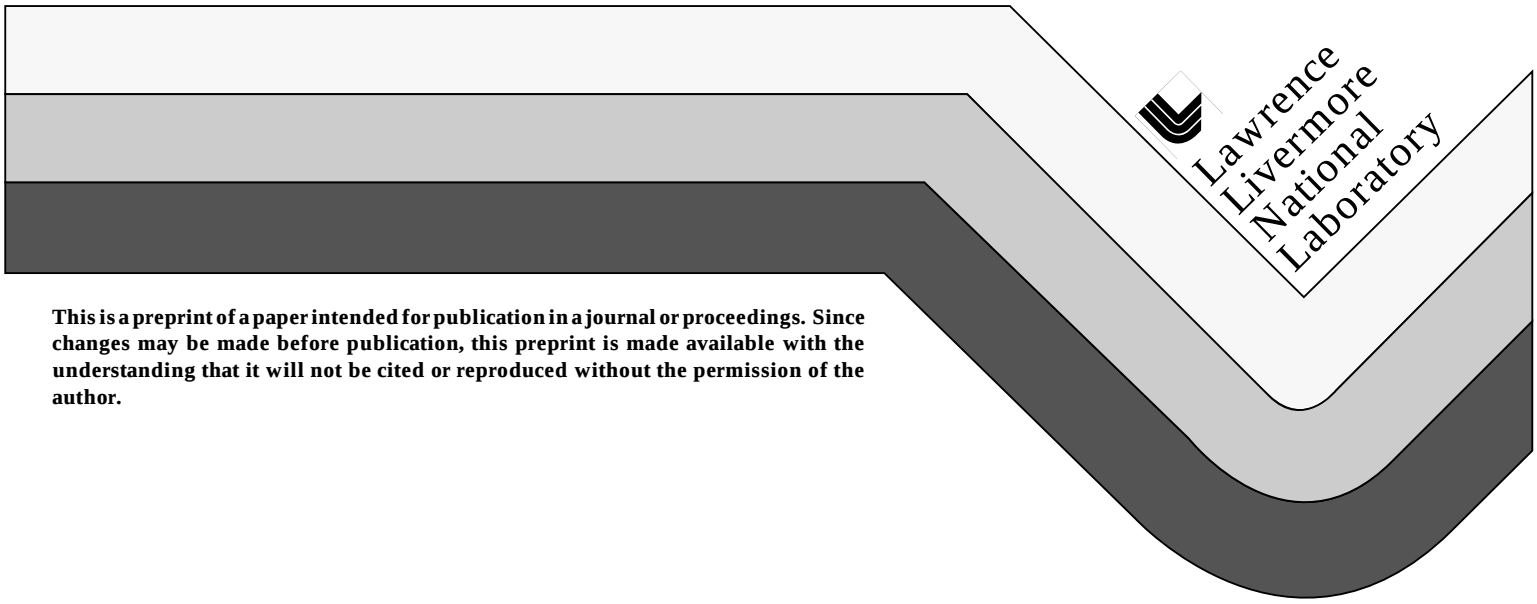
UCRL-JC-119743
PREPRINT

Firewall Products Today

S.P. Cooper

This paper was prepared for submittal to the
DOE Computer Security Group Training Conference
Milwaukee, WI
May 2-5, 1995

February 1995



Firewall Products Today

Stephen P. Cooper
Computer Security Technology Center
Lawrence Livermore National Laboratory[1]
Email: spcooper@llnl.gov

Abstract

With an increased interest in connecting to the Internet, there is a corresponding interest in protecting an organization's network from others on the Internet. Internet firewalls help protect an organization's network, and the increased demand for firewalls have brought about a number of freeware and commercial products. But how does someone determine the best product or service for their organization?

This paper discusses things that need to be considered in deciding to build or purchase a firewall system. It discusses many of the products, features, and services that are commercially available[2] and what components they include such as software, hardware, consulting, or a combination thereof. This paper is not an attempt to evaluate the products. The aim is to provide an awareness of what is currently available and their capabilities. An appendix gives contact information for all of the vendors whose product information was used in developing this paper.

Introduction

As more computers and larger networks get attached to the Internet, it gets more difficult to protect an organization's information and resources from others on the Internet. An increasingly popular method of connecting to the Internet is through firewalls. A well constructed firewall can be quite effective in protecting an organization's information and resources, while still providing access to many of the services available on the Internet.

A firewall is a combination of hardware and software components that provide a single point-of-control between a "trusted" network, such as an organizational network, and an "untrusted" network such as the Internet (see Figure 1). The firewall provides a certain level of control as to what occurs between the two networks. There are several ways to make your own firewalls, and there are a number of people and companies providing firewall consulting. Additionally, there have been a number of commercial firewall products being announced or released.

---

[1] This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National laboratory under contract No. W-7405-Eng-48.

[2] Reference to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by U.S. Department of Energy or the University of California.

Firewalls are not only for connecting to the Internet. They can be used between almost any two networks with different security policies. The firewall serves as a gateway between the networks and helps protect the networks from each other. For example, a network with sensitive research and development information or personnel information can be protected from the rest of an organization while still providing electronic mail exchange throughout the organization.

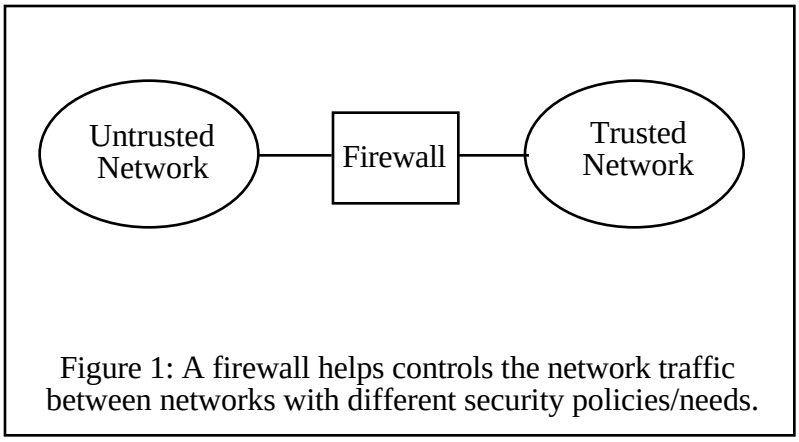


Figure 1: A firewall helps controls the network traffic between networks with different security policies/needs.

For a firewall to function, it must be able to make decisions on all of the data that passes through it. It passes the data that the policy says may pass and blocks the data that shouldn't. The actual implementation is much more difficult, because network applications are frequently designed for functionality, not security.

Firewall Overview

Security Policy

A firewall is a tool for enforcing *security policy*. Cheswick and Bellovin [CHES94] state that "a security policy determines the limits of acceptable behavior, and what the response to violations should be." The firewall helps enforce the limits established by the security policy as it relates to network activity that passes through the firewall.

Of course, a firewall can only be effective on the network traffic that passes through it. If there are other paths into your network, such as via modem pools, they must also fall into the bounds set by the security policy.

A firewall is an effective means for protecting a network. However, current firewall technology can only reduce, not eliminate, the threat to your information and resources. Firewalls, like the systems they protect, are built from complex combinations of software and hardware. They also require some level of system configuration and administration. Bugs in the software or mistakes in administration can open security holes through the firewall and leave a network vulnerable to attack. Additionally, users, intentionally or unintentionally, may open up security holes. For example,

a user may hook up a modem on the inside of the firewall, thus creating the possibility of bypassing the firewall.

Whenever we discuss firewalls, we want to stress that user education and host-based security are important elements in enforcing security policy. As demonstrated in Figure 2, the firewall serves as the first line of defense. With the additions of good host security and user education, we can vastly reduce the threat to our information and resources.

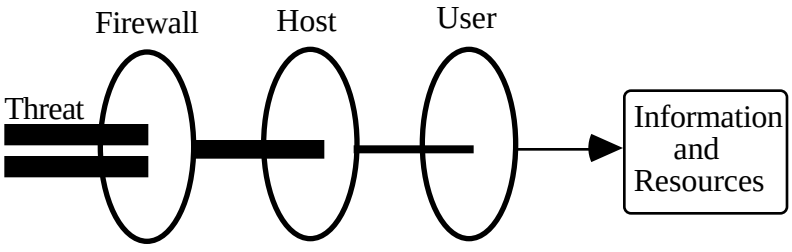


Figure 2: The firewall works together with host security and user education to reduce the threat to information and resources.

We have been looking at firewalls for the protection of inside information and resources. Firewalls are also useful for controlling the access to external services and networks. For example, some organizations limit who may send mail or transfer files outside of an organization.

Firewall Components

A firewall system consists of a number of hardware and software components. What components are included may vary depending on who is building or supplying the firewall. A *router* is used to connect two networks together. Its primary purpose is to limit the traffic crossing a network boundary to that whose destination is across the boundary. *Screening routers,* also known as *packet filtering routers*, have more control over the traffic that passes through them. By defining a **s***creening table* or *access control list* (ACL), packets can be dropped based on the protocol type, source or destination address or port, direction of connection, etc.

For some sites and policies, a screening router is sufficient for firewall protection. However, there are limitations that quickly make the screening router insufficient for certain sites. One of the limitations is the difficulty of getting the screening tables correct on some routers. A mistake here can leave your network wide open.

The *application gateway,* also called a *Bastion Host*, offers a higher level of control. The application gateway is a host machine that runs programs that forward and filter connections for services such as TELNET and FTP. The application gateway usually serves as the host that is logically exposed to the less trusted network. The firewall is set up so that application protocols cannot get to an inside host unless they pass through the appropriate application proxy on the gateway. Furthermore, the protocol cannot get through unless the proxy exists to pass it through. The

proxy may perform *secure authentication* during a connection establishment or perform extra logging. The purpose of secure authentication is to avoid sending reusable passwords over the network where they can be *snooped*. There are several forms of secure authentication systems available. Some require each user to have a special card which may cost as much as $50.00 each or more. There is free software, such as S/Key from Bellcore, which uses a challenge/response mechanism. A firewall may support one or more secure authentication systems.

Firewall Configurations

The firewall components are combined into a number of possible configurations (see Figure 3). As mentioned earlier, the screening router is suitable for some small sites but is often missing features such as logging and secure authentication.

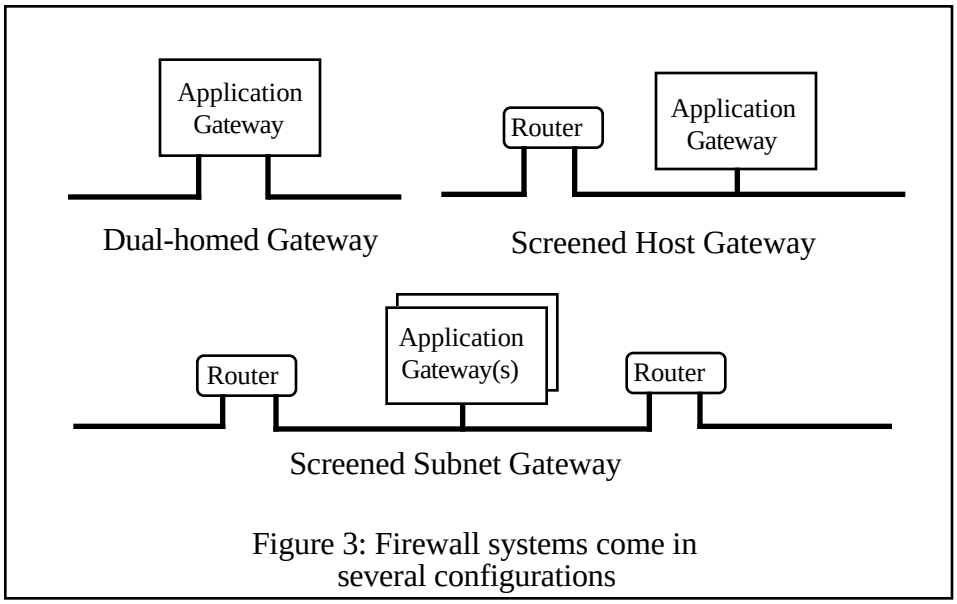


Figure 3: Firewall systems come in several configurations

The *dual-homed gateway* is an application gateway with two network interfaces and IP forwarding disabled. All traffic must pass through some kind of proxy or filter implemented in software on the gateway. This system is relatively simple to build and requires a minimum of hardware. Because of that, it is a popular configuration for commercial vendors of firewall software or systems.

The *screened host gateway* combines a packet filtering router with an application gateway. The application gateway may be on the inside or on the outside of the router. If on the inside, the router only permits traffic to that host from the outside. If on the outside, the router only permits certain traffic from that host. The router may pass through traffic for applications that are considered trustworthy. The problem with this configuration is that it shares some of the disadvantages of using a screening router as the firewall, such as the difficulty in managing it and properly setting up its tables. The Checkpoint Firewall-1 offers an option that integrates the management of Cisco routers into the firewall management.

The *screened subnet gateway* uses a second screening router to create a small isolated network between the trusted network and the untrusted one. The routers direct traffic such that the application gateway(s) on the screened subnet are the only ones accessible from either side of the network. This offers the ability to have multiple application gateways on the screened subnet. On large networks, this could be useful for dividing the proxy work such as using FTP on one, mail on another, etc. It also offers the capability to hide network addresses on one side of the firewall from the other side. This makes probing more difficult. On the down side, it further adds to the difficulty of administration.

Other configurations are possible. Also, application gateway and screening router features offered by the respective vendors are moving closer. Some dual-homed gateway firewalls include packet filtering features. Some router vendors are adding better logging and secure authentication features to their screening routers.

The Firewall Lifecycle

The firewall lifecycle includes preparation, specification and procurement, installation, maintenance, and, if you are properly paranoid, a lot of second-guessing and re-evaluation.

Preparation

When do you prepare for a firewall installation? You start when you plan to connect two networks with different security policies and needs. Or, if you already have two such networks connected together, you realize that there may be threats to the information and resources on one of the networks from the other. In other words, the roots of your information security requirements are in your business plan and based on a realistic risk assessment.

Training is another important part of preparation. Even if you go with commercial information security products and services, information security is an integral part of your business and not something you can completely turn over to a third party. You need to have some knowlege of the issues so that you can effectively work with the vendor and monitor the vendor's performance. There are books and seminars available on firewalls and information security, as well as information available via the World Wide Web. Many vendors also offer training.

The primary output of this phase is the security policy. It is important to remember that the security policy should determine the firewall requirements. The firewall is to help support the policy, not impose one.

Specification and Procurement

In this phase the security policy is mapped to the firewall requirements and configuration and a selection is made for the hardware and software to satisfy the requirements. Specification and procurement are put together because it is a tightly coupled cyclical process where you may need to update the specification for what is available. For example, some people

want their firewall to be a Windows NT box, but there are no currently available firewalls in that configuration.

When specifying your firewall, you may want to consider what resources you have available. This includes personnel as well as hardware. You may have existing equipment that you want to use for your application gateway or screening routers. Your personnel may be familiar with a particular vendor's version of the UNIX operating system, upon which most application gateways are built.

This is the phase where you want to decide whether to purchase commercial products or services or build you own. We will discuss those options later.

Installation

This will vary depending on your network and firewall configurations. The important things are that you want to test it as much as possible, to verify that blocked services are blocked and allowed services get through. If you are replacing a previously unsecured or less secure network connection, you may want to check the previously "exposed" hosts with a security tool such as the Security Profile Inspector (SPI).

Maintenance

The amount of maintenance a firewall requires depends on its configuration. The components, such as routers and application gateways, may require periodic system patches and updates. Most important are security patches that are put out by the system vendors. These are often referenced in CIAC bulletins. The bulletins should be monitored regularly for items that may pertain to your firewall.

Another factor effecting firewall maintenance is the amount of auditing or logging requested. These logs have to be checked and purged. Some firewalls offer the option of sending the logs to another machine to be checked. The Internet Site Patrol includes a service where your logs are encrypted and sent offsite to their location for analysis and 24-hour incident response.

Other maintenance items are the number and types of protocols you allow, the complexity and frequency of changes in your network, and the complexity of your configuration for dealing with the changes.

Re-evaluation

As we have already shown under maintenance, a firewall is not something you install and forget. New and sophisticated threats are always surfacing. CIAC Advisory F-08 (January 23, 1994) discussed an Internet address spoofing attack that was capable of penetrating some firewalls. CIAC Advisory F-11 (February 14, 1994) discussed a vulnerability with the NCSA WWW server software (httpd). You need to be aware of these new threats and be sure you are protected. If you are using a commercial product or service, is the vendor keeping up with the threats and modifying your firewall in response? As your business changes and evolves, is your security policy and therefore your firewall staying in line with the changes?

A good way to stay current in firewall information is to subscribe to and monitor the firewall mailing list. This contains a lot of discussion and pros and cons of different protocols, configurations, and products. However, the list is fairly busy and likely to get more so.

Firewall Products

Building Your Own

There is free software available to help build a firewall. However, it is not trivial and it takes a certain amount of expertise in several areas, including computer network security, UNIX system administration, and programming.

TIS Firewall Toolkit

A popular, free software toolkit for building firewall systems is the Firewall Toolkit from Trusted Information Systems, Inc. (TIS). This kit provides the tools for building a firewall, most specifically an application gateway. It includes proxies for TELNET, FTP, and http. It also provides tools for incorporating strong user authentication and for securing SMTP-based mail. Frederick Avolio of TIS, in a posting to the Firewall Toolkit users' mailing list, sums the expertise needed as follows:

> *The FWTK is meant for individuals who:*
> *- know C*
> *- know TCP/IP*
> *- know UNIX as a system manager*
> *- have built C software packages on UNIX systems*

One of the advantages of the Firewall Toolkit is that it comes in source form and has been ported to a number of different UNIX operating systems and versions.

Socks

Socks is a package used to build circuit relays. It replaces standard system calls so that their TCP/IP connections pass through the gateway machine. A disadvantage to this is that the network applications on the host machines have to be linked to the socks library in order to utilize the gateway.

Screend

This is a package that allows you to build a packet filter out of a UNIX system. It requires that you have the kernel source code.

KarlBridge

This is a package that allows you to build a filtering router out of a PC with two network interfaces such as two Ethernet cards.

Related Software

There is other free software available for firewall use. These include proxies such as *xforward* for X11 and a http proxy from CERN. A popular free secure authentication package is *S/Key* from Bellcore. These can often be used as add-ons or replacements for Firewall Toolkit components.

Commercial Services

Internet providers

One possible source for firewall functionality could be the Internet provider that supplies your connection to the Internet. They may be able to provide some filtering capabilities customized to your needs. In fact, as competition heats up among the Internet providers, and threats continue to be publicized, security may be a value-added service offered by many Internet providers.

Consultants

There are many security and network consultants and consulting organizations that will build a firewall for you. Some may use or recommend a commercial product while others may construct one for you from the previously mentioned free software. Many of the consultants may also help you analyze your overall security needs and help you define policy.

Commercial Products

With the rising popularity of the Internet, there have been a number of new commercial firewall products being produced or announced. Many of them attempt to make it easier to configure and maintain a firewall. One general goal is to approach a turn-key system. This goal is still far off due to a number of reasons. The first reason is that organizations have different security policies and needs. Their network configurations are different and contain a different mix of systems and protocols. This makes it very difficult to build a *one size fits all* firewall system. Here we'll look at some of the features provided by different firewall systems.

Protocols

Most firewall systems work with IP because it is the primary protocol used on the Internet. The filtering router capabilities handle IP, TCP, and UDP by source and destination addresses and source and destination ports. The application gateway capabilities do higher level application filtering for TELNET, FTP, and others. Some routers have filtering capabilities for other, usually Ethernet-based protocols. The KarlBridge, for example, has filtering capabilities for DECnet packets (address, Area, Object number, and Object name), AppleTalk Phase 1 & 2 NBP packets (file server name, printer name, and/or Zone name), and Novell SAP packets (Network number, Server name, and Service).

Hardware and Operating Systems

All of the firewall vendors supply firewall software. They vary as to whether or not they include the hardware and/or operating system. Firewall-1 is a software product for Sun platforms. JANUS includes software and a hardened UNIX operating system targeted for a 486/33 (minimum) platform with two network interfaces. The hardware is not included.

Some firewall systems are commercializations of the TIS Firewall Toolkit. TIS, itself, has produced Gauntlet, a commercial version of its toolkit. Gauntlet includes a security modified version of BSDI UNIX and the hardware. BSDI UNIX is a popular operating system for commercial firewalls because it is a robust, well supported system and the sources are relatively inexpensive. The sources are modified by the vendor to make the system more secure.

One thing to remember when considering firewall systems is that, as a choke point between networks, a firewall may also be a single point-of-failure if a hardware or software component fails. The cost, availability, and speed of repair may be an important consideration.

Management

Other features include better management interfaces. Firewall-1 provides an X-Windows based user interface for its management functions. It also provides the capabilities to generate router command lists for downloading to some makes of packet filtering routers. The use of an X-Windows user interface has raised concerns among some security professionals due to the increased complexity and security problems with the X-Windows system.

User Authentication

Firewalls that provide some inbound access, such as an employee telecommuting via TELNET from home, incorporate some type of secure authentication in their system. This prevents the use of reusable passwords across an unsecured network. There are several different authentication systems available. Firewall products may support one or more of the systems, so this is a consideration when selecting a firewall product.

Encryption

Some organizations need to communicate securely and privately over an untrusted network such as the Internet. There are some router products available where a secure, encrypted *channel* is established with a similar router. LanGuardian examines outgoing packets and encrypts them if they are destined to certain addresses where another LanGuardian decrypts the message. Packets destined to public places are not encrypted. Network Systems' Data Privacy Facility takes this further, by encrypting packets based on source and destination address and port, security label, protocol type, and packet length. With it, multiple *sleeves* may be established between sites with more control over the packet flow.

Firewall Validation

A critical part of building or purchasing a firewall is verifying that it works and is secure. There are two parts to this. First the hardware, software, and operating system components have to be capable of being secure if properly configured. Secondly, once installed and configured, the firewall has to be secure and support the security policy.

How can a firewall vendor provide assurance that the components they are providing are secure? The philosophy behind TIS's Firewall Toolkit is that the source is available and is small enough for inspection. They have continued this philosophy with their commercial firewall system, Gauntlet. Secure Computing (SCC) has taken a different approach for its announced, but not yet released Sidewinder product. They have broadcast a challenge on the Internet where there are prizes for those who can break into their firewall.

An installed firewall is much more difficult to validate. That is because the interaction of components adds much more complexity. A proxy may be very secure, but it is useless if a router is configured to bypass the application gateway for the application protocol. In the case of testing by the vendor, that test configuration and environment probably differs from the one at the customer's site. One possibility for installed firewall testing is through *white hat* vulnerability services. This is where you arrange for a trusted party to attempt to break into your network and provide you with their results. There are some security consultants who can provide this service. White hat testing is also available from the Computer Security Technology Center through CIAC or the Secure Systems Services project.

Services

Firewall vendors often provide related services, either as part of their product or as additional consulting. This includes help in evaluating security needs and in developing security policy. It also includes training in information security and in the use and maintenance of their products.

As mentioned earlier, the Internet Site Patrol offers a unique firewall monitoring service. With this service, the firewall encrypts and sends logging information to their site for 24-hour analysis and incident response.

Some firewall products are actually services in which the vendor builds a firewall system for you. Digital Equipment Corporation's SEAL (Screening External Access Link) is such a service.

Conclusion

There are many things to think about when building or purchasing a firewall system. The rate of growth of the Internet and the security service and product industry mainly serves to add to the confusion. There are many good products out there. You just have to pick the product or service that best fits your requirements and budget.

References and Resources

Here are some resources used for this paper and useful for getting started on firewalls. The firewall mailing list is a good source for up-to-date information and discussion on firewall related security issues. There is also some discussion and critique of commercial products. Some of the commercial vendors maintain their own mailing lists.

The Computer Security Technology Center and the Computer Incident Advisory Capability will continue to monitor the technology and products for information security. In addition, the Secure Systems Services project can provide consultation for information security needs. For more information, see the CIAC home page at *http://ciac.llnl.gov.*

[CHES94] Cheswick, William R. and Steven M. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley, 1994. *Firewalls and Internet Security* has become the de facto reference book for firewalls and contains much useful information and an extensive bibliography.

[WACK94] Wack, John P. and Lisa J. Carnahan. Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls. National Institute of Standards and Technology, Draft 1994.

Firewalls Mailing List. E-mail subscription requests to *firewalls-request@greatcircle.com* with "subscribe firewalls" as the message body.

Catherine Fulmer maintains a WWW page of commercial vendors at http://www.digimark.net/bdboyle/fulmer/firewall.vendor.html.

Appendix A: Firewall Products and Vendors

Information regarding the following products was used to develop this paper. Due to the fact that some products are available through multiple vendors, the list is organized alphabetically by product name. Due to the rapid expansion in the firewall industry, the information presented here is sure to be obsolete as soon as it is written.

Black Hole

Company: Milkyway Networks Corporation
WWW: http://www.milkyway.com/
Contact: Send electronic mail to *info@milkyway.com* or call (Canada) 613-566-4574.
Comments:

Cyberguard

Company: Harris Computer Systems
WWW:
Contact: Send electronic mail to *nhnews@csd.harris.com* or call 305-974-1700 Ext. 5144 for Sales or Ext. 5124 for Marketing.
Comments: Custom software, hardware, and operating system. The operating system and hardware are "NCSC B1-level evaluated and ITSEC FB1 E3 secure."

Data Privacy Facility

Company: Network Systems Corp.
WWW: http://www.network.com
Contact: Phone 612-424-1488.
Comments: Packet-based encrypting router.

Eagle Network Security Management System

Company: Raptor Systems
WWW: http://www.delmarva.com/raptor/raptor.html
Contact: Call 617-487-7700.
Comments: Software package that runs on an IBM, Hewlett-Packard, or Sun Microsystem workstation.

Firewall-1

Company: Checkpoint Software
WWW: http://WWW.CheckPoint.com
Contact: Send electronic mail to *sales @CheckPoint.com.* Also available through multiple distributers.
Comments: Software that runs on Sun workstations. Provides packet filtering as well as application gateway capabilities.

Gauntlet

Company: Trusted Information Systems, Inc. (TIS)
WWW: http://www.tis.com/
Contact: Send electronic mail to *etsec@tis.com,* call 301-854-6889, or fax 301-854-5363.
Comments: TIS provides the free Internet Firewall Toolkit. Gaunlet is based on the toolkit and is built on a UNIX operating system modified to increase security.

InterLock$_{SM}$ Security Services

Company: Advanced Network & Services, Inc.
WWW:
Contact: Send electronic mail to *info@ans.net* or call 800-456-8267
Comments: Annual service including hardware, software, initial configuration, and maintenance. Runs on an IBM RS/6000 320 running modified AIX 3.1.5

IRX Router

Company: Livingston Enterprises
WWW:
Contact: Phone 800-458-9966 or e-mail info@livingston.com
Comments: Packet filtering router with logging and some application gateway features.

JANUS™ (JANOS, BorderWare) Firewall Server

Company: Border Network Technologies
WWW: http:///www.border.com
Contact: Multiple resellers available. Contact Border Network Technologies (Canada) at 416-368-7157, or *sales@border.com.*
Comments: Software and operating system with GUI administration interface. Operating system is a hardened UNIX system for Intel 486/33 (minimum) platform with two network interfaces. Harware not included.

KarlBridge

Company: Karlnet Inc. (US) or Sherwood Data Systems Ltd. (UK).
WWW: http://www.gbnet.net/kbridge/
Contact: In U.S. phone KarlNet Inc. at 614-263-KARL or e-mail sales@KarlNet.com. In U.K. phone Sherwood Data Systems Ltd. at 44-(0)1494-464264 or e-mail sales@gbnet.com.
Comments: Software that runs on a 286/386/486 clone to build a multi-protocol filtering router. Also available with hardware. Shareware demo versions are available via anonymous FTP.

NetGate

Company: SmallWorks of Travis Co.
WWW:
Contact: Phone/fax to 512-338-0619 or e-mail info@smallworks.com
Comments: Software for Sun SPARC systems running SunOS 4.1.X. Provides packet filtering, logging, and forwarding. Available in both binary and source distributions.

NetSP

Company: IBM
WWW:
Contact: Phone 919-254-7416 or 919-254-6898, fax 919-254-4239, or e-mail sbaumann @ vnet.ibm.com
Comments: Firewall software for IBM Risc System/6000 computers with AIX 3.2.5.

PORTUS

Company: Livermore Software Labs
WWW:
Contact: Phone 800-240-5754 or e-mail portusinfo@gw.lsli.com
Comments: Firewall software for IBM RS/6000.

SEAL

Company: Digital Equipment Corporation
WWW: http://www.digital.com/info/seal.html
Contact: Phone Dick Calandrella at 508-496-8626.
Comments: Service which will build a custom firewall system on DEC computers.

SecurityGate

Company: Digital Equipment Corporation
WWW:
Contact: Any local DEC office about DEC SecurityGate for OpenVMS, Version 1.1.
Comments: Software for OpenVMS DECnet Phase IV routing node provides additional access control.

Sidewinder™

Company: Secure Computing Corporation
WWW: http://www.sctc.com
Contact: Phone 800-692-5625 or e-mail sidewinder@sctc.com
Comments: Unreleased product based on type enforcement.

SITE PATROL

Company: BBN Internet Services Corp.
WWW: http://www.near.net/bbnisc/site.patrol/site.patrol-page.html
Contact: Phone BBN BARRNET Inc. (CA) at 415-725-1790 or BBN NEARNET Inc. (MA) at 1-800-NEARNET or 617-873-8730.
Comments: PC-Based Bastion Host and router with dual-Ethernet connections. Includes monitoring and incident response services.

Technical Information Department • **Lawrence Livermore National Laboratory**
University of California • Livermore, California 94551